YEAR 2000 COMPLIANCE EFFORT
AT THE
OFFICE OF THRIFT SUPERVISION

OIG-99-022 DECEMBER 23, 1998

Office of Inspector General

****

United States Department of the Treasury

MEMORANDUM FOR ELLEN SEIDMAN, DIRECTOR
OFFICE OF THRIFT SUPERVISION

FROM: David C. Williams
Inspector General

SUBJECT: Year 2000 Compliance Effort at the Office of
Thrift Supervision

This memorandum presents the results of our assessment of the Office of Thrift Supervision's (OTS) Year 2000 conversion effort. We performed a limited review of this effort. In addition to the OTS, the Office of Inspector General (OIG) evaluated and reported on the Year 2000 efforts at other Treasury bureaus individually, as well as from a Department-wide perspective. Subsequent work may be performed by us in the future and will be reported to you in a separate report.

Overall, we concluded that the OTS established an infrastructure for managing its conversion effort and minimizing the risk that a Year 2000 induced failure would have on its mission critical operations. No significant reportable issues came to our attention. However, the inherent nature of the Year 2000 dilemma denies the ability to completely eliminate risk. The Year 2000 problem comes with inherent risks that all organizations face and will continue to face, despite their best efforts and demonstrated success. Accordingly, we developed three suggestions encouraging OTS, as well as other Treasury bureaus, to sustain efforts in the areas of change management, data exchange, and contingency planning for business continuity to minimize potential disruptions caused by these inherent risks.

Although an official written response was not required because we made no recommendations for corrective action, OTS provided their comments to our draft report. The OTS generally concurred with the OIG findings and suggestions, and any technical clarification provided by OTS was incorporated as appropriate. The full text of OTS' response is included as Appendix 1.

OBJECTIVES, SCOPE, AND METHODOLOGY

Our overall objective was to evaluate OTS' internal Year 2000 conversion effort for its mission critical information technology (IT) systems. Our specific objectives were to evaluate the following: (1) project management; (2) system conversion and certification; and (3) contingency plans for business continuity. In addition, we performed a limited review of OTS' Year 2000 strategy and progress for non-IT and telecommunications systems.

Our review was limited to evaluating strengths and weaknesses in the management of the Year 2000 conversion project. Specifically, we determined if processes existed and were designed to mitigate the Year 2000 risk to an acceptable level for ensuring all mission critical IT systems remain operable. Therefore, this memorandum is not intended to represent or convey statements that any given system is Year 2000 compliant or that a system will or will not work into the next millennium.

From June through August 1998, using a risk based audit approach, we reviewed and evaluated applicable Year 2000 documentation, including: Treasury's Year 2000 Vulnerability Assessment Report, dated October 1997; OTS' monthly status reports; OTS' Year 2000 Project Plan, and other related documents. In addition, we interviewed the appropriate officials within OTS that had responsibility for the Year 2000 project, and we met with the General Accounting Office (GAO) auditors to discuss the results of their previously performed OTS Year 2000 audit work.

AUDIT RESULTS

Overall, we concluded that OTS established an infrastructure for managing its conversion effort and minimizing the risk that a Year 2000 induced failure would have on its mission critical operations. OTS' project management and strategies for conversion, testing, and contingency planning were adequate to address their needs. No significant reportable issues came to our attention. However, we made three suggestions which may assist the OTS, as well as other bureaus, in sustaining their Year 2000 efforts. Details on the results of our assessment, and our suggestions and OTS' response to these suggestions are provided below.

Project Management

OTS demonstrated a high level of awareness and dedication to its conversion effort. The majority of costs associated with the conversion effort related to OTS' oversight function of the thrift industry. OTS was renovating its systems and using date expansion to the four digit year, as prescribed by Treasury's date standard. Of the 15 mission critical IT systems at OTS, 13 have been repaired and implemented with the final systems scheduled for implementation in late 1998.

System Conversion and Certification Process

OTS' Year 2000 conversion process and certification plans were comprehensive and set forth clear certification criteria. Notable efforts were the extensive end to end testing, multiple certification testing, and the involvement by system owners in the testing of these systems. For certification, OTS established a schedule of five time periods that certification testing would take place. Depending on the work load during a scheduled time, certification may be performed several times. By final certification, OTS expected that each mission critical system will have been certified at least twice.

Aside from the positive efforts noted above, we are making the following suggestions for management to consider. As part of managing the Year 2000 conversion risk to an acceptable level, strong change management controls for conversion integrity and continued coordination with data exchange partners are two areas we believe warrant mentioning.

Ensuring Year 2000 Conversion Integrity

It is important for OTS to ensure that subsequent modifications and environmental changes do not nullify certified test results. Generally, the risk that a system may fail due to system changes increases as January 1, 2000 approaches and the time available for additional testing decreases. The risk associated with modifying a system will vary depending on the timing and complexity of the changes. The closer system changes occur to the end of testing and certification, the higher the risk. Additionally, the more applications, programs, and interfaces affected by a specific change, the higher the risk to conversion and testing integrity. As organizations complete system, integration, and end to end testing, the likelihood increases that even small changes subsequent to these tests could jeopardize the integrity of certification. Business users and management both have critical roles for managing the risk of system changes. They both need to evaluate potential changes in the context of Year 2000 compliance, and balance the risk to operations of not implementing a change with the risk of rendering a system non-Year 2000 compliant.

One suggested practice to mitigate conversion risk is to adopt "freeze policies," or as done by the Federal Reserve, put in place a "limitation window and moratorium policy[1]." Whether an organization opts for a complete restriction or limited restriction, it is critical that the timing of such a policy is driven by test schedules and progress. The more systems that are tested and certified as Year 2000 compliant, or the more aggressive the existing test schedule is, the lower the tolerance should be for approving changes.

Suggestion

1. We suggest that the OTS Director ensures a disciplined change management process continues to maintain Year 2000 conversion integrity. Once a system has been certified, steps need to be taken to ensure test integrity is maintained. Subsequent changes, including platform upgrades, software enhancements, or any system modification should be evaluated and approved with the understanding of

[1] Terms adopted from the Federal Reserve's century date change management policy. The limitation window is the period where there is a higher standard for requesting and approving system changes. A moratorium would occur towards the end of the limitation window, closer to January 1, 2000, and would further restrict changes.

> the implications. This could be accomplished by establishing specific criteria for approving system changes. Criteria should address such factors as: nature, timing, and extent of requested change; documented assessment of requested change; extent of retesting required; and number of organizations and partners affected.
>
> In response to this suggestion, OTS stated that additional testing during 1999 will help ensure that changes to the system, the operating environment and external interfaces have not impacted OTS' Year 2000 readiness. Year 2000 testing of the client server platform and the automated Report of Examination will be conducted in 1999. Subsequent modifications to systems and the platform will be reviewed by OTS' Year 2000 IT team to assess the readiness risk.

Coordinating Pivots With Data Exchange Partners

Notable efforts at OTS include the thorough care in managing its interface inventory and coordinating with its data exchange partners. OTS identified its data exchange partners and mission critical and non-mission critical interfaces. The majority of the mission critical interfaces were compliant. Bridges were developed, tested, and implemented for the non-compliant interfaces. OTS contacted all of its external exchange partners and reached agreements on the resolution of any problems.

Nonetheless, for exchange partners using a windowing logic technique in lieu of a four digit field expansion, special care needs to be given to coordinate pivots.[2] For example, all Treasury bureaus exchange payroll, budget, and accounting data with the Financial Management Service (FMS) which uses the windowing logic technique. If exchange partners choose different pivots, the century identifiers could be incorrectly inferred if further processing, calculating, or sorting is performed on data transferred. For example, if OTS is using a pivot date of 50 and its exchange partner is using a pivot date of 60, date values in between 1950 through 1960 and 2049 through 2059 could be calculated in error. Without coordination with exchange partners, bureaus may not adequately develop and test new data exchange formats, nor apply the necessary bridges and filters to ensure the exchanges will function properly. The greater the number and complexity of data exchanges, the greater the challenge in identifying, synchronizing, and testing exchange formats.

<u>Suggestion</u>

[2] The windowing logic technique uses pivots to interpret a two digit year into a four digit year. All year values above the pivot are understood to represent one century; while all values below the pivot are understood to represent another century. Pivots refer to a number built into system logic to infer the 2 digit century identifier "19" or "20". For example, a pivot of 50 infers 19 as the century identifier for values 50-99 and infers 20 for values 0-49.

2. We suggest that the OTS Director ensures data exchange procedures continue to identify and coordinate pivot dates with its exchange partners. Where there are differences in pivot dates, OTS should ensure that filters are installed to synchronize and maintain the accuracy of century identifiers. This is especially important between processing partners, i.e., those partners whose data is transferred for further processing.

   In response to this suggestion, OTS stated that it continues to monitor the Year 2000 compliance status of its external interfaces. Additionally, OTS contacted FMS to ascertain the certification test plans and will continue to work with FMS to ensure the exchange will function properly.

Contingency Plans for Business Continuity

OTS progressed significantly over the last few months in preparing business continuity plans. OTS established clear guidance, expectations, and milestone dates for business users with the responsibility for developing these plans. These plans were due for OTS management review in September 1998. As of the end of our field work, these plans were still being reviewed by OTS management and were not available for our evaluation.

It is management's responsibility to reduce the risk of Year 2000 related failures and maintain a minimum acceptable level of service. Contingency planning is required to assure continuity of operations in the event of an unanticipated Year 2000 failure, and for systems that will not be Year 2000 compliant. Contingency planning should address risks not only with internal systems, but external risks with business partners and the public infrastructure. Plans should identify resources, procedures, and appropriate training required to carry out core business functions. Plans should clearly identify triggers for implementation, be tested thoroughly, and continuously reevaluated. Steps should be included that facilitate the restoration of normal services at the earliest possible time.

Suggestion

3. We suggest that the OTS Director ensures that management prioritizes and facilitates the preparation and testing of contingency plans for each core business function, as well as mission critical systems. As part of managing the development and potential implementation of these plans, management should ensure that: these plans consider both the internal and external risks; resources and implementation triggers are identified; training in executing the plan is performed; and the plans are periodically evaluated for reasonableness.

   In response to this suggestion, OTS stated that it planned to develop contingency plans later than recommended by GAO guidance. OTS' approach called for developing contingency plans after validation/certification testing took place. This has enabled the Year 2000 compliance status of the system, its dependencies, and the validation testing results to be considered when assessing the risk for contingency planning.

We appreciate the courtesies and cooperation provided to our auditors during the audit. If you wish to discuss this report, you may contact me at (202) 622-1090 or a member of your staff may contact Barry L. Savill, Director of Audit at (202) 283-0151.

cc: Treasury Departmental Offices
Assistant Secretary for Management and Chief Financial Officer
Deputy Assistant Secretary for Information Systems
and Chief Information Officer
Assistant Director of Information Technology Policy and Management
Director, Office of Organizational Improvement
Director, Office of Strategic Planning
Director Financial Management Division
Office of Budget
Desk Officer, Management and Controls Branch
Desk Officer, Office of Accounting and Internal Control

Office of Thrift Supervision
Cora Prifold Beebe, Executive Director of Administration
Arthur Oliver, Bureau OIG Liaison

Office of Management and Budget
Michael S. Crowley, Budget Examiner

MANAGEMENT RESPONSE

Office of Thrift Supervision *Ellen Seidman*
Department of the Treasury *Director*
1700 G Street, N.W., Washington, DC 20552 • (202) 906-6590

December 3, 1998

MEMORANDUM FOR: Dennis Schindel
Assistant Inspector General for Audit

FROM: Ellen Seidman

SUBJECT: Year 2000 Compliance Effort at the Office of Thrift Supervision (A-DO-98-014)

I am in receipt of the draft results of your assessment of the OTS Year 2000 conversion effort. Your positive feedback on OTS' internal Year 2000 conversion effort for its mission critical information technology systems confirms our view that we have diligently responded to the challenges to information technology posed by the Year 2000 date conversion.

As of October 6, 1998, OTS completed renovation, testing, and implementation of all fifteen mission critical systems and they have been tested for Year 2000 compliance at the OTS Remote Disaster Recovery Center in Philadelphia. Year 2000 IT Contingency Plans have been developed for each mission critical system to help OTS prepare for the continuity of critical services. The OTS Business Recovery Team is reviewing the Year 2000 IT Contingency Plans to identify areas of concern regarding the program, the costs, or the availability of resources. A contingency plan for telecommunications is being developed based on guidance provided by the Department of Treasury and is scheduled to be completed by year-end.

Ensuring Year 2000 Conversion Integrity

To ensure Year 2000 conversion integrity, OTS has budgeted two additional tests at the Remote Disaster Recovery Center in 1999 to retest the mission critical systems. The second round of testing during 1999 will help ensure that changes to the system, the operating environment and external interfaces have not impacted our Year 2000 readiness. Year 2000 testing of the client server platform and the automated Report of Examination will be conducted in 1999. Subsequent modifications to systems and the platform will be reviewed by the Y2K IT team to assess the risk to our Year 2000 readiness.

MANAGEMENT RESPONSE

Coordinating Pivots With Data Exchange Partners

On Page 4, I recommend replacing the last two sentences in the first paragraph under the pivot topic with the following:

> Bridges have been developed where necessary for both temporary and permanent interfaces. OTS continues to monitor the Year 2000 compliance status of its external interfaces.

Regarding the second paragraph under **Coordinating Pivots With Data Exchange Partners**, OTS does not use pivot dates. OTS complied with Treasury's requirement to convert to a four-digit year for all bureau data that is shared with other government agencies or with the private sector. Based on Treasury Financial Manual Bulletin No. 98-06, FMS payment applications will function with a two-digit year. To accommodate this requirement, OTS converts the four-digit year back to a two-digit year for FMS tape processing. We have contacted FMS to ascertain their certification test plans for processing a two-digit year in a simulated Year 2000 environment and will continue to work with them to ensure the exchange will function properly. OTS does not use the National Finance Center for payroll or accounting processing.

Contingency Plans for Business Continuity

On Page 5, I recommend deleting the second sentence and the first word of the third sentence.

OTS did not view contingency planning as unnecessary. Rather, OTS planned to develop contingency plans later than recommended by GAO guidance. Our approach called for developing contingency plans after validation/certification testing took place. This has enabled the Y2K compliance status of the system, its dependencies and the validation testing results to be considered when assessing the risk for contingency planning.

I appreciate the opportunity to provide comments. If you wish to discuss them, please contact either me or OTS' IG liaison, Arthur Oliver, who can be reached on 906-7956.